PIERCE O'DONNELL (SBN 081298)
PODonnell@GreenbergGlusker.com
TIMOTHY J. TOOHEY (SBN 140117)
TToohey@GreenbergGlusker.com
PAUL BLECHNER (SBN159514)
PBlechner@GreenbergGlusker.com
GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590
Telephone: 310.553.3610
Fax: 310.553.0687

Attorneys for Plaintiff
MICHAEL TERPIN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

MICHAEL TERPIN,

Plaintiff,

v.

AT&T MOBILITY, LLC; and DOES 1-25,

Defendants.

Case No. 2:18-cv-06975-ODW-KS

EXHIBIT TO PLAINTIFF'S OPPOSITION TO THE MOTION TO DISMISS OF DEFENDANT AT&T MOBILITY, LLC

[Fed. R. Civ. Proc. 12(b)(6)]

Assigned to:
Honorable Otis D. Wright II

Hearing: December 3, 2018
Time: 1:30 p.m.
Dept./Place: 350 West 1st Street, 5th Floor, Courtroom 5D, Los Angeles, CA 90012

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

EXHIBIT TO PLAINTIFF'S OPPOSITION TO THE MOTION TO DISMISS THE COMPLAINT OF DEFENDANT AT&T MOBILITY, LLC

For the convenience of the Court, attached as Exhibit A hereto is *In the Matter of Cox Communications, Inc.*, 30 FCC Rcd. (2015).

DATED: September 5, 2018

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By: /s/ Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff MICHAEL TERPIN

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

30 FCC Rcd. 12302 (F.C.C.), 30 F.C.C.R. 12302, 63 Communications Reg. (P&F) 1064, 2015 WL 6779864

Federal Communications Commission (F.C.C.)
Order

IN THE MATTER OF COX COMMUNICATIONS, INC.

File No.: EB-IHD-14-00017829
Acct. No.: 201632080001
FRN: 0001834696
DA 15-1241
Released: November 5, 2015
Adopted: November 5, 2015

**1 *12302 By the Chief, Enforcement Bureau:

1. **Consumers** of **cable** and **satellite** services are entitled to have their **personal information** protected. The Communications Act already imposes heightened obligations on cable and satellite operators to protect the personally identifiable information of their subscribers, and to take such actions as are necessary to prevent unauthorized access to this information. Inadequate security of subscribers' personal information can result in real world consequences for those customers, who are put at risk of financial and digital identity theft. In the wrong hands, a customer's sensitive personal information could also be used to take control of a customer's real accounts, to change the passwords on those accounts, to expose the customer's personal information on the web, and to harass or embarrass the customer through social media. Today, the Enforcement Bureau (Bureau) of the Federal Communications Commission has entered into a Consent Decree to resolve its investigation into whether Cox Communications, Inc. (Cox), failed to properly protect the confidentiality of its customers' proprietary information (PI), proprietary network information (CPNI), and personally identifiable information, and whether Cox failed to promptly notify law enforcement authorities of security breaches involving CPNI, as required by Commission rules (Rules).

2. Cox's electronic data systems were breached in August 2014 when a third party used a common social engineering ploy known as pretexting. Specifically, the third party pretended to be from Cox's information technology department and gained access to data systems containing Cox customer information by convincing a Cox customer service representative and a Cox contractor to enter their respective account IDs and passwords into a fake website, which the third party controlled. The relevant data systems did not have technical safeguards, such as multi-factor authentication, to prevent the compromised credentials from being used to access the PI and CPNI of Cox's customers. Thus, the third party was able to make use of the credentials to view personal data of Cox's current and former customers, including sensitive personal information such as name, home address, email address, phone number, partial Social Security Number, partial driver's license number, and telephone customers' account-related data. This third-party hacker then posted some of the personal information of at least eight of the affected customers on social media sites, changed the passwords of at least 28 of the affected customers, and shared customer personal information with another alleged hacker. Cox did not report the breaches through the Commission's breach-reporting portal.

**2 3. Congress and the Commission have made clear that cable operators such as Cox must "take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[1] Furthermore, telecommunications carriers such as Cox must take *12303 "every reasonable precaution"[2] to protect their customers' data. In addition, the law requires carriers to promptly disclose CPNI breaches via our reporting portal within seven (7) business days after reasonable determination of a breach to facilitate the investigations of the FBI and the United States Secret Service.[3]

4. To settle this matter, Cox will pay a civil penalty of $595,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into Cox's business practices to protect consumers against similar data breaches in the future. In particular, Cox will be required to improve its privacy and data security practices by: (i) designating

a senior corporate manager who is a certified privacy professional; (ii) conducting privacy risk assessments; (iii) implementing a written information security program; (iv) maintaining reasonable oversight of third party vendors, to include implementing multi-factor authentication; (v) implementing a more robust data breach response plan; and (vi) providing privacy and security awareness training to employees and third-party vendors. Cox will also identify all affected consumers, notify them of the breach, provide them with free credit monitoring, and file regular compliance reports with the FCC.

5. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding Cox's compliance with Sections 201(b), and 222(a) and (c), and 631(c) of the Communications Act of 1934, as amended (Act), as well as Sections 64.2010(a) and 64.2011(b) of the Rules.[4]

6. In the absence of material new evidence relating to this matter, we do not set for hearing the question of Cox's basic qualifications to hold or obtain any Commission license or authorization.[5]

7. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act[6] and the authority delegated by Sections 0.111 and 0.311 of the Rules,[7] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

8. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED.**

12304 9. **IT IS FURTHER ORDERED that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Barry Ohlsohn, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., 975 F Street, NW, Suite 300, Washington, DC 20004, and to counsel David H. Solomon, Esq., and J. Wade Lindsay, Esq., Wilkinson Barker Knauer, LLP, 1800 M Street, N.W., Suite 800N, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

**3 Travis LeBlanc
Chief
Enforcement Bureau

12305 CONSENT DECREE

1. The Enforcement Bureau of the Federal Communications Commission and Cox Communications, Inc. (Cox), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether Cox violated Sections 201(b) and 222(a) and (c), and 631 of the Communications Act of 1934, as amended, and Sections 64.2010(a) and 64.2011(b) of the Commission's rules.[1]

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:
(a) "Act" means the Communications Act of 1934, as amended.[2]

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any Customer whose PI and/or CPNI was viewed by unauthorized third parties in connection with the August 7, 2014, data breach.

**4 (d) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(e) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(f) "Communications Laws" means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which Cox is subject by virtue of its business activities.

(g) "Compliance Officer" means the individual designated in paragraph 16 of this Consent Decree as the person responsible for administration of the Compliance Plan.

(h) "Compliance Plan" means the compliance obligations, programs, and procedures described in this Consent Decree at paragraph 17.

(i) "Covered Employees" means all employees of Cox assigned to call centers that provide customer service or sales service for Cox Customers managed and operated by Cox, Cox field technicians, and Cox information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of, duties that involve access to, use, or disclosure of PI and/or CPNI. Covered Employees do not include Covered Third Party Employees.

(j) "Covered Third Party" means any third-party that, on behalf of Cox, operates and/or manages a call center that provides customer service or sales service for Cox, ***12306** provides field technician services, or provides information technology Help Desk services.

(k) "Covered Third Party Employees" means all employees of Covered Third Parties assigned to call centers that provide customer service to Cox Customers, field technicians, and information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of PI and/or CPNI of Cox Customers.

(l) "Cox" means Cox Communications, Inc., its wholly owned subsidiaries that own and operate cable systems that provide video, broadband, or telecommunications services in the United States and successors-in-interest.

(m) "Customer" means any current and/or former subscriber of any Cox service, which service is subject to the Communications Laws. "Customer" shall include any applicant for any Cox service to the extent that Cox, or any Covered Third Party collects and stores PI and/or CPNI regarding the applicant on behalf of Cox, in any Cox or Covered Third Party electronic data systems.

(n) "Customer Proprietary Network Information" or "CPNI" shall have the meaning set forth at 47 U.S.C. § 222(h).

(o) "Effective Date" means the date by which the Bureau and Cox have signed the Consent Decree.

(p) "Investigation" means the investigation commenced by the Bureau in File No. EB-IHD-14-00017829 regarding whether Cox violated the Privacy Laws in 2014.[3]

****5** (q) "Operating Procedures" means the standard internal operating procedures and compliance policies established by Cox to implement the Compliance Plan.

(r) "Parties" means Cox and the Bureau, each of which is a "Party."

(s) "Personal Information" or "PI" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit ***12307** card number, in combination with any required security code, access code, PIN, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(t) "Privacy Laws" means Sections 47 U.S.C. §§ 201(b), 222, and 551, and 47 C.F.R §§ 64.2001-2011, insofar as they relate to the security, confidentiality, and integrity of PI and/or CPNI.

(u) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

II. BACKGROUND

3. Section 631(c) of the Act provides that, with certain exceptions, a cable operator "shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[4]

4. Section 222 of the Act is entitled "Privacy of customer information."[5] Section 222(a), entitled "In general," provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to ... customers."[6] The Commission has interpreted Section 222(a) as applying to customer ""proprietary information" that does not fit within the statutory definition of CPNI.[7] The Commission has stated that proprietary information broadly encompasses all types of information that should not be exposed widely to the public, whether that information is sensitive for economic or personal privacy reasons,[8] and that this includes privileged information, trade secrets, and personally identifiable information.[9]

5. Section 222(c) of the Act imposes certain restrictions on telecommunications carriers to protect the confidentiality of their customers' CPNI.[10] Section 64.2010(a) of the Rules establishes protections for CPNI by requiring carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.[11] Section 64.2011(b) requires carriers to provide notification of a CPNI breach via the FCC portal "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach."[12]

**6 6. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service *12308 [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.""[13] The Commission has interpreted Section 201(b) to apply to carriers' data-security practices for protecting proprietary information.[14] In that regard, the Commission has interpreted Section 201(b) to require companies to employ just and reasonable data security practices to protect consumers' proprietary information.[15]

7. Cox provides digital cable television services, broadband Internet access service, telecommunications services, and home automation services in the United States. Cox is the third largest cable company in the United States, serving approximately six million residential and commercial customers,[16] and is the seventh largest landline telephone provider in the United States.[17]

8. The Bureau's review of the record shows that Cox's systems were breached on or about August 7, 2014, by a hacker using the alias "EvilJordie," a member of the hacker group known as the Lizard Squad.[18] This individual apparently used a social engineering method known as pretexting[19] to gain access to Cox electronic data systems containing customer information. Specifically, EvilJordie pretended to be from Cox's information technology department and convinced a contractor to enter her account ID and password into a fake, or "phishing," website on or about August 7, 2014.[20] According to Cox, the phony phishing website appeared to be a Cox website but, in fact, was controlled by "EvilJordie."[21] Around the same time, the access credentials of a Cox Tech Support representative were also compromised by means of a social engineering effort that prompted the representative to enter his access credentials into the same phishing website. Cox states that it believes that ""EvilJordie" shared the compromised credentials with "chF."[22]

9. As a result of these actions, the hackers had access to Cox electronic data systems that included some PI of *** active Customers and some PI and CPNI of *** telephone *12309 Customers.[23] The record reflects that from August 7, 2014, through August 14, 2014, the hackers viewed some PI of 54 current Affected Customers, seven former Affected Customers, and likely viewed some CPNI of at least one, but possibly up to four, of these Affected Customers.[24] The hackers posted some information of eight of the Affected Customers on social media sites; they also changed the passwords of 28 of the Affected Customers' whose PI was viewed.[25] Of the current Affected Customers whose information was viewed, 20 subscribed to telephone service at the time of the breach.[26]

**7 10. Cox asserts that it learned of the August 7th breach on August 12, 2014, when a Cox employee in San Diego received an email from a Nevada Customer who complained of account information being posted on a social media site.[27] Cox's privacy team then engaged its customer safety team, which investigated the incident, identified the source of the breach, and

WESTLAW © 2018 Thomson Reuters. No claim to original U.S. Government Works.

disabled the compromised access credentials within two days of learning of the August 7th breach. At the time of the breach, Cox employed multi-factor authentication for some employees and third party contractors with access to Cox electronic data systems, but not for the compromised employee or contractor. Cox's internal policies and training programs expressly prohibited Cox employees and third party contractors from disclosing access credentials to anyone and warned against pretexting attacks. On August 18, 2014, Cox directly contacted the FBI and cooperated in the subsequent investigation of the breach, which resulted in the arrest of "EvilJordie."[28] Cox did not disclose the CPNI breach via the FCC data breach reporting portal. Via a letter dated September 16, 2014, Cox notified all but two of current Affected Customers that their PI/CPNI had been compromised as a result of a Cox customer service representative sharing access credentials with an unknown individual and offered free credit monitoring services.[29] Cox took other remedial steps as a result of the incident.

11. The Bureau subsequently commenced an investigation that it states involved whether Cox: (i) failed to properly protect the confidentiality of Customers' personally identifiable information; (ii) failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI; (iii) failed to provide timely notification to law enforcement of a CPNI breach; and (iv) engaged in unjust and unreasonable practices by (a) failing to employ reasonable data security practices to protect proprietary information and CPNI, and failing to monitor for Customers' breached data online; and (b) failing to notify all potentially affected Customers of the breaches. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

12. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order without change, addition, deletion, or modification.

13. **Jurisdiction**. Cox agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

*12310 14. **Effective Date**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

8 15. **Termination of Investigation. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation. In consideration for the termination of the Investigation, Cox agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute, on its own motion, any new proceeding, formal or informal, or take any action on its own motion against Cox concerning the matters that were the subject of the Investigation. The Bureau also agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute on its own motion any proceeding, formal or informal, or to designate for hearing the question of Cox's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations.[30]

16. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, Cox shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer, together with the Chief Privacy Officer (who shall be privacy certified by an industry-certifying organization and who shall keep current through appropriate continuing privacy education courses) and Chief Information Security Officer, shall be responsible for developing, implementing, and administering the Compliance Plan, including the Information Security Program (as defined in paragraph 17(b)) required under the Compliance Plan, and ensuring that Cox complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of the Privacy Laws relevant to their duties, prior to assuming their duties.

17. **Compliance Plan**. For purposes of settling the matters set forth herein, Cox agrees that it shall, within one hundred twenty (120) calendar days after the Effective Date, supplement its existing compliance policies and procedures regarding the Privacy Laws by developing and implementing a Compliance Plan designed to ensure future compliance with the Privacy Laws, and with the terms and conditions of this Consent Decree, which shall be implemented and operated in accordance with Cox's risk-based approach. Such Compliance Plan must include the following components:
9 (a) **Risk Assessment. Cox shall conduct a comprehensive and thorough risk assessment, conducted with reference to the NIST Cybersecurity Framework, to identify internal and external risks to the security, confidentiality, and integrity of PI/CPNI collected or maintained by Cox or Covered Third Parties that could result in unauthorized access, disclosure, misuse, destruction, or compromise of such information (Risk Assessment). The Risk Assessment, which shall be completed no later than December 31, 2016, must evaluate in writing the likelihood and potential impact of these threats and the sufficiency of existing policies, procedures, and other safeguards in place to control risks. Additional Risk Assessments shall be conducted at least biennially and Cox shall notify the Commission of completion of the Risk Assessments within thirty (30) calendar days via e-mail to the persons listed in paragraph 19(d).

*12311 (b) **Information Security Program**. Within one hundred fifty (150) calendar days after the Effective Date, Cox shall review and revise as appropriate its information security program to ensure that, using a risk-based approach, it has a reasonable and comprehensive security program to protect the security, confidentiality, and integrity of PI and CPNI collected and/or maintained by Cox or Covered Third Parties (Information Security Program). Cox shall ensure that such Information Security Program is documented in writing (including, as appropriate, within the Operating Procedures and Compliance Manual described below) and includes:
i. Administrative, technical, and physical safeguards that are reasonable in light of Cox's size and complexity, the nature and scope of Cox's activities, the sensitivity of the PI/CPNI collected or maintained by or on behalf of Cox, and the risks identified through risk assessments, including the use of multiple factor authentication or equivalent control(s) for Covered Employees' access to PI/CPNI;

ii. Reasonable measures to protect PI/CPNI collected or maintained by Covered Third Parties, including exercising due diligence in selecting Covered Third Parties, where reasonably feasible requiring Covered Third Parties by contract (upon execution of new agreements and renewal agreements) to implement and maintain reasonable and comprehensive safeguards of both the physical and electronic protection of PI/CPNI equivalent to the safeguards used by Covered Employees (e.g., with regard to multiple factor access/authentication or equivalent control(s) to Cox data systems/Customer information), engaging in appropriate verification of Covered Third Parties' compliance with their security obligations, and implementing appropriate measures to sanction Covered Third Parties that fail to comply with their security obligations (including, where appropriate, terminating Cox's relationship with such Covered Third Parties); and

iii. Policies and procedures to properly identify the nature and extent of CPNI and PI collected or maintained by Cox and Covered Third Parties, minimize the number of Employees who have access to PI and CPNI on a strictly need-to-know basis tied to job functions, collect the minimum amount of PI necessary to provision and provide services, and collect and maintain PI in a manner that is secure.

**10 In addition, and in accordance with its risk-based approach, Cox shall:
iv. Review and evaluate periodically the effectiveness of the Information Security Program's key controls, systems, and procedures particularly with regard to how such controls, systems, and procedures impact compliance with the Privacy Laws;

v. Monitor critical points within Cox's infrastructure containing PI and CPNI for security events. This process includes taking information feeds from industry sources and internal detection tools (e.g., antivirus) and correlating these information sources to alert Cox's security monitoring center when a potential event has occurred. The security monitoring team will take action on alerts as necessary;

vi. Adjust and update its Information Security Program as appropriate in light of limitations and deficiencies indicated by the reviews, evaluations, and monitoring described herein; and

*12312 vii. Conduct annual audits of selected call center systems and processes using procedures and standards generally accepted in the profession, to ensure compliance with the Privacy Laws and this Consent Decree. The audits may be performed by Cox Enterprises Inc.'s Audit Services team (which operates separately from Cox) and which itself and through a co-sourcing relationship with a large global external audit firm, which Cox represents has the requisite knowledge and information-security related certifications including but not limited to: Certified Information Security Auditor; Certified Information Systems Security Professional; Certified Privacy Technologist; Certified Risk and Information Systems Control; Certified Fraud Examiner; and Certified Internal Auditor. Systems and processes shall be selected for audit based on Cox's risk evaluations and prioritization. Cox will notify the Commission of the completion of the audits within thirty (30) days via e-mail to the persons listed in paragraph 19(d).

viii. Conduct annual penetration testing of selected systems and processes related to payment cards and collection and storage of PI/CPNI. Systems and processes shall be selected for testing based on Cox's reasonable risk evaluations and prioritization.

ix. Develop an approach to internal threat monitoring that includes the detection of anomalous conduct by Covered Employees no later than December 31, 2016 and begin implementing such approach within one hundred twenty (120) days of that date.

(c) **Third Party Oversight**. Within one hundred twenty (120) calendar days after the completion of the Information Security Program, Cox shall implement the provisions of paragraph 17(b)(ii). In addition, Cox shall require all off-network access by Covered Third Parties with access to Cox customer PI/CPNI to be authenticated through an approved site-to-site virtual private network by December 31, 2016. Furthermore, by the first quarter of 2016, Cox shall conduct a formal assessment by a third party consulting firm to identify additional two-factor authentication opportunities, and by the end of the first quarter of 2016 shall complete the migration of all Covered Third Parties with access to Cox customer PI/CPNI leveraging remote access Citrix platforms to a two-factor authentication solution.

11 (d) **Incident Response Plan. Within one hundred and twenty (120) calendar days after the Effective Date, Cox shall review, revise and maintain its Incident Response Plan to ensure that it is reasonable, comprehensive, and enables Cox to detect, respond to, and provide timely notification, in accordance with the Privacy Laws, applicable law, and the requirements of subpart 17(e) below, to all relevant Customers and relevant governmental authorities of data breaches involving PI and CPNI. Such Incident Response Plan shall contain processes to (i) identify, (ii) investigate, (iii) mitigate, (iv) remediate, and (v) review information security incidents to identify root causes and to develop improved responses to security threats. Cox shall perform annual test exercises of the Incident Response Plan, and shall subject such plan to third-party review.

(e) **Breach Notification**. Within one hundred and twenty (120) calendar days after the Effective Date, and periodically thereafter, Cox shall review its breach notification practices to ensure that, to the extent they do not already so provide, in the event of an unauthorized breach of Customer PI/CPNI, Cox shall: (i) at least to the extent required by federal or state law, or guidance from law enforcement, notify all Customers (at the Customer's last known address and pursuant to Cox's reasonable *12313 efforts to locate the Customer) whose unredacted and/ or unencrypted PI/CPNI information has been, or for which Cox knew, acquired by an unauthorized person; (ii) offer complimentary credit monitoring service for a minimum of one year to any Customer whose unredacted and/or unencrypted PI/CPNI is reasonably believed by Cox to have been acquired by an unauthorized person and if, consistent with industry practices, Cox reasonably believes involves a risk of identity theft; and (iii) conduct targeted monitoring of known websites for breach activity to identify potential Customer PI/CPNI data. Cox shall ensure that policies and statements on Cox's websites regarding the security of Customers' PI and CPNI accurately reflect Cox's data security practices, and are updated routinely to reflect any material changes.

(f) **Remediation Measures**. To the extent that Cox has not previously satisfied the requirements set forth below, within one hundred and twenty (120) calendar days after the Effective Date, unless otherwise indicated, Cox shall, with respect to the breach that was the subject of the Investigation:
i. Continue conducting targeted monitoring of known websites for breach activity to identify potential Affected Customer PI/CPNI data;

ii. Offer to provide one year of complimentary credit monitoring services to all Affected Customers through a nationally

recognized credit monitoring service, the availability of which must be described in the notice discussed below; and

iii. Identify each Affected Customer and ensure that each Affected Customer has been notified (at the Customer's last known address and pursuant to Cox's reasonable efforts to locate the Customer) that his or her PI and/or CPNI was compromised. The notification to each Affected Customer must include:
**12 a. A general description of the manner in which the Affected Customer's PI/CPNI was compromised;

b. A general description for all Affected Customers of the type of PI/CPNI that was compromised;

c. The toll-free telephone numbers and addresses of the major credit reporting agencies;

d. Information regarding the complimentary credit monitoring services available to Affected Customers;

e. A toll-free hotline or website where Affected Customers may contact Cox to inquire about their compromised PI, and receive reasonable and comprehensive counseling on responding to and mitigating credit harm incidences, including identity theft; and

f. Reasonable and comprehensive information regarding free and/or readily available credit protection options including obtaining free annual credit reports, placing fraud alerts on credit files, requesting security freezes, contacting financial institutions, and any other such free and/or readily available credit protections.

(g) **Notice of Consent Decree**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall deliver a copy of this Consent Decree to all existing Covered Employees, and shall also deliver a copy of this Consent Decree to all future Covered Employees within sixty (60) calendar days after the person assumes such *12314 position or responsibilities. The Consent Decree can be delivered together with the Compliance Manual as provided in subpart 17(i) below.

(h) **Operating Procedures**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall establish Operating Procedures that all Covered Employees must follow to help ensure Cox's compliance with this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(g) of this paragraph, and the Privacy Laws. Cox shall also develop a compliance checklist that describes the key steps that a Covered Employee must follow to ensure compliance with this Consent Decree and the Privacy Laws.

(i) **Compliance Manual**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall review, revise, use, and maintain a Compliance Manual (which may be in hard copy and/or electronic format). Within the same period, Cox shall distribute the Compliance Manual to all Covered Employees and to each Covered Third Party, requesting, and, where permitted by contract, requiring the Covered Third Party to distribute the Compliance Manual to each Covered Third Party Employee. For any person who becomes a Covered Employee more than one hundred twenty (120) calendar days after the Effective Date, Cox shall distribute the Compliance Manual to that person within sixty (60) calendar days after the date such person becomes a Covered Employee, and prior to such person engaging with Customers with respect to Cox's services. Further, Cox shall request, and where permitted by contract, require each Covered Third Party to distribute the Compliance Manual to each person who becomes a Covered Third Party Employee more than one hundred twenty (120) calendar days after the Effective Date within sixty (60) calendar days after such person becomes a Covered Third Party Employee, and prior to such person engaging with Customers with respect to Cox's services.
**13 i. The Compliance Manual shall set forth and explain the requirements of the Privacy Laws and this Consent Decree, and shall instruct Covered Employees to ensure Cox's compliance with the Privacy Laws and this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(h) of this paragraph. Cox shall request, and where permitted by contract require, Covered Third Parties to direct Covered Third Party Employees to consult and follow the Operating Procedures.

ii. The Compliance Manual shall require Covered Employees to contact their supervisor or the Compliance Officer with any questions or concerns that arise with respect to Cox's obligations under or compliance with the Privacy Laws and this

Consent Decree, and require any supervisor who receives such information from a Covered Employee or Covered Third Party Employee to promptly notify the Compliance Officer. Cox shall request, and where permitted by contract require, Covered Third Parties to provide appropriate mechanisms for Covered Third Party Employees to contact their supervisor with any questions or concerns that arise with respect to their obligations under or compliance with the Privacy Laws and this Consent Decree, and for any such supervisor who receives such information from a Covered Third Party Employee to promptly notify the Compliance Officer. Cox shall provide and request, and, where permitted by contract, require Covered Third Parties to provide a hotline or other appropriate mechanism for anonymous reporting of any noncompliance.

***12315** iii. Cox shall review and revise the Compliance Manual to ensure that the information set forth therein remains current and complete.

iv. Cox shall distribute any revisions of the Compliance Manual to all Covered Employees and Covered Third Parties within sixty (60) calendar days after any revisions have been made by Cox. These revisions may be in electronic format.

(j) **Compliance Training Program**. Within six months after the Effective Date, Cox shall review, revise, implement, and maintain a compliance training program to ensure compliance with the Privacy Laws and this Consent Decree. In addition, Cox shall request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees receive training in accordance with the Compliance Training Program:
i. The Compliance Training Program shall include reasonable and comprehensive privacy and security awareness training for all Covered Employees. The program shall include instruction on Cox's obligations, policies, and procedures for protecting PI and CPNI pursuant to the Privacy Laws and this Consent Decree, including identifying and collecting PI from Customers, recognizing security threats and suspicious activity that may indicate that PI has been compromised, the timely reporting of data breaches, and other reasonable and appropriate training regarding the protection of PI and CPNI. Cox shall cause all Covered Employees whose job functions relate to the implementation of the remediation measures described in paragraph 17(f) to receive training regarding such remediation measures, as described below. For purposes of complying with the provisions of this paragraph, Cox is permitted to provide the training or use a third party to provide the training described herein.

****14** ii. As part of the Compliance Training Program, Cox shall ensure that each Covered Employee is advised of Cox's obligations to report any noncompliance with the Privacy Laws and this Consent Decree, and is instructed on how to disclose noncompliance to the Compliance Officer, including instructions on how to anonymously report such noncompliance. Cox shall request, and where permitted by contract, require, Covered Third Parties to disseminate the same instructions to each Covered Third Party Employee.

iii. Cox shall ensure that the training for Covered Employees is conducted pursuant to the Compliance Training Program within six (6) months after the Effective Date, except that any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within sixty (60) calendar days after the date such person becomes a Covered Employee. Cox shall document its Covered Employees' completion of the training. Cox shall request, and where permitted by contract, require all Covered Third Parties to conduct the same type of training for each of their Covered Third Party Employees within the same period, and to document completion of that training.

iv. Within one hundred eighty (180) calendar days after the Effective Date, Cox shall not allow any Covered Employee to interact with any Customer about Cox's service until the Covered Employee has been ***12316** trained and has received a copy of the Compliance Manual. Beginning within one hundred eighty (180) calendar days after the Effective date, Cox shall further request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees shall not interact with any Customer about Cox's service until their Covered Third Party Employees have been trained consistent with this subparagraph 17(j); and

v. Cox shall ensure that the Compliance Training Program is conducted at least annually for Covered Employees. Cox shall request, and where permitted by contract, require Covered Third Parties to ensure that the Compliance Training Program is conducted at least annually for Covered Third Party Employees. Cox shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

18. **Reporting Noncompliance**. Cox shall report any material noncompliance with the Privacy Laws, and the terms and conditions of this Consent Decree, within fifteen (15) calendar days after discovery by the Compliance Officer, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that Cox has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) the steps that Cox has taken or will take to prevent the recurrence of any such noncompliance. Cox shall also report to the FCC any breaches of PI or CPNI involving any Covered Employees or Covered Third Party Employees that Cox is required by any federal or state law to report to any Federal or state entity or any individual. Reports shall be submitted no later than seven (7) business days after completion of the notification required by Federal or state authorities. Such reports shall include: (i) the date the breach was reported; (ii) the applicable Federal and state authorities to whom the breach was reported; (iii) copies of the reports Cox submitted to the applicable Federal and state authorities; and (iv) the reference number generated by the central reporting facility for CPNI reports made pursuant to 47 C.F.R. § 64.2011(b). All reports of noncompliance or PI/CPNI breaches shall be submitted to the Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with a copy submitted electronically to David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@fcc.gov.

15 19. **Compliance Reports. Cox shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.

(a) Each Compliance Report shall include a detailed description of Cox's efforts during the relevant period to comply with the terms and conditions of this Consent Decree and the Privacy Laws. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of Cox, stating that the Compliance Officer has personal knowledge that Cox: (i) has established and implemented the Compliance Plan required by paragraph 17; (ii) has utilized the applicable Operating Procedures since the implementation of the Compliance Plan; and (iii) is not aware of any instances of material noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 18 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the *12317 Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[31]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of Cox, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of such noncompliance; (ii) the steps Cox has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that Cox has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

(d) All Compliance Reports shall be submitted to the Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with copies submitted electronically to Jennifer.Lewis@fcc.gov, Dana.Leavitt@fcc.gov, Kenneth.Scheibel@fcc.gov, and David.Roberts@fcc.gov.

20. **Termination Date**. Unless stated otherwise, the obligations set forth in paragraphs 18 and 19 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The obligations set forth in paragraphs 16, 17(a) and 17(b) shall expire seven (7) years after the Effective Date. The obligations set forth in paragraphs 17(c)-(j) shall expire six (6) years after the Effective Date.

21. **Section 208 Complaints; Subsequent Investigations**. Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act[32] against Cox for alleged

violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from investigating new evidence of noncompliance by Cox with the Communications Laws.

16 22. **Civil Penalty Cox shall pay a civil penalty to the United States Treasury in the amount of Five Hundred Ninety-five Thousand dollars ($595,000.00) (Civil Penalty). Cox shall send electronic notification of payment to Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission at Jeffrey.Gee@fcc.gov, David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@fcc.gov, on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[13] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:
· Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

· *12318 . Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

· Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank —Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES @fcc.gov.

23. **Waivers**. As of the Effective Date, Cox waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. Cox shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither Cox nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and Cox shall waive any statutory right to a trial *de novo*. Cox hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[14] relating to the matters addressed in this Consent Decree.

17 24. **Severability. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

25. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

26. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this Consent Decree to which Cox does not expressly consent) that provision will be superseded by such Rule or Order.

27. **Limitation**. The definitions and terms set out in this Consent Decree are intended solely for this Consent Decree and not as an extension or limitation of the Privacy Laws.

28. **Successors and Assigns**. Cox agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

29. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

30. **Modifications**. This Consent Decree cannot be modified without the advance written consent of all Parties.

***12319** 31. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

32. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

33. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____

Travis LeBlanc, Chief

Enforcement Bureau

_____

Date

_____

Jennifer W. Hightower

Senior Vice President and General Counsel

Cox Communications, Inc.

_____

Date

Footnotes

1 47 U.S.C. § 551(c)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12525 para. 24 n.61 (1996) ("[I]n the Cable Communications Policy Act of 1984, Congress ... sought to restrict unauthorized use of personably identifiable information [PII] by cable operators.").
The Cable Act generally prohibits the disclosure of PII unless such disclosure is necessary to render the services requested or for a legitimate business activity related to such service. *See 47 U.S.C. § 551(c)(2)(A). See also id.* §§ 201, 222(a), (c); 47 C.F.R. § 64.2010.

2 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007).

3 *See* 47 C.F.R. § 64.2011(b).

4 *See* 47 U.S.C. §§ 201, 222(a), (c); 47 C.F.R. §§ 64.2010, 64.2011.

5 *See* 47 C.F.R. § 1.93(b).

6 47 U.S.C. § 154(i).

7 47 C.F.R §§ 0.111, 0.311.

1 47 U.S.C. §§ 201(b), 222(a) and (c), 551; 47 C.F.R. §§ 64.2010(a) and 64.2011(b).

2 47 U.S.C. § 151 *et seq.*

3 *See, e.g.*, Letter from Jeffrey J. Gee, then-Acting Chief, Investigations and Hearings Division, Enforcement Bureau to Barry J. Ohlson, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., (Feb. 12, 2015) (on file in EB-IHD-14-00017829). Cox responded to that letter and subsequent requests for information, and Cox requested confidential treatment of specified information contained in its responses (including material contained in the accompanying exhibits) pursuant to Sections 0.457 and 0.459 of the Rules. *See* 47 C.F.R. §§ 0.457, 0.459. Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox, to Jennifer A. Lewis, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (Mar. 16, 2015) (on file in EB-IHD-14-00017829) (LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 4, 2015) (on file in EB-IHD-14-00017829) (Supplemental LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 20, 2015) (on file in EB-IHD-14-00017829). Because we do not disclose material Cox identified as confidential, we defer ruling on the requests unless and until necessary. *See* 47 C.F.R. § 0.459(d)(3) (permitting deferred rulings until a request for inspection has been made pursuant to Sections 0.460 or 0.461 of the Rules; such materials will be accorded confidential treatment until the Commission acts on such requests and all subsequent appeal and stay proceedings have been exhausted).

4 47 U.S.C. § 551(c)(1).

5 *See id.* § 222.

6 *Id.* § 222(a).

7 *See, e.g., Terracom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330-13332, paras. 14-19 (2014) (citing *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6745 para. 207 (2012)) (*Terracom NAL*), *settled by TerraCom, Inc. and YourTel America, Inc.*, Order and Consent Decree, 30 FCC Rcd 7075 (Enf. Bur. 2015).

8 *Id.*

9 *Id.* at 13331, para. 17.

10 *See* 47 U.S.C. § 222(c).

11 *See* 47 C.F.R. § 64.2010(a).

12 *Id.* § 64.2011(b).

13 47 U.S.C. § 201(b).

14 *Terracom NAL*, 29 FCC Rcd at 13335-36, paras. 31-32.

15 *Id.*

16 Cox Communications Fact Sheet, http://newsroom.cox.com/company-overview (last visited Nov. 3, 2015).

17 *See* Cox Communications Digital Telephone Fact Sheet, http://newsroom.cox.com/product-fact-sheets (last visited Nov. 3, 2015).

18 *See* LOI Response at 1-2, 8-10.

19 "Pretexting" is a form of misrepresentation whereby the perpetrator adopts the identity of a legitimate person or entity to obtain confidential and personal information belonging to the targeted individual. *See* Federal Bureau of Investigation, "Owner, Employee, and Contractor of Private Investigative Firm Sentenced in Connection with Pretexting" (Dec. 14, 2012), https://www.fbi.gov/sanfrancisco/press-releases/2012/owner-employee-and-contractor-of-private-investigative-firm-sentenced-in-connection-with-pretexting.

20 *See* LOI Response at 1-2, 8-9. "Phishing" is the deceptive use of an identity that appears to come from a legitimate, well-known source in order to trick an individual into divulging sensitive or personal information, such as account numbers or passwords, often through a link to a copycat of the purported source's Web site. *See* Federal Trade Commission, FTC Issues Staff Report on Roundtable Discussion About Phishing Education (Jul. 14, 2008), https://www.ftc.gov/news-events/press-releases/2008/07/ftc-issues-staff-report-roundtable-discussion-about-phishing.

21 LOI Response at 1-2, 8-9.

22 *See* LOI Response at 1-2, 8-10. The Bureau's review of the record also shows that a single Cox subscriber reported a possible incident by a hacker using the alias "chF," (an apparent member of the Lizard Squad) to Cox on July 22 and 31, 2014. *See, e.g.*, LOI Response at Bates # 00643-48, 01640-41.

23 *See* Supplemental LOI Response at 8-9.

24 *See* LOI Response at 2; Supplemental LOI Response at 10. No credit card information could have been viewed and only the last four digits of the Social Security number and driver's license number, not the entire Social Security or driver's license number, could have been viewed. LOI Response at 11; Supplemental LOI Response at 8-9.

25 *See* Supplemental LOI Response at 2.

26 *Id.*

27 *See* LOI Response at 9-10.

28 *See id.* at 9-10; 17-18.

29 *See id.* at 14.

30 *See* 47 C.F.R. § 1.93(b).

31 *See* 47 C.F.R. § 1.16.

32 47 U.S.C. § 208.

33 An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

34 *See* 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501-1.1530.

30 FCC Rcd. 12302 (F.C.C.), 30 F.C.C.R. 12302, 63 Communications Reg. (P&F) 1064, 2015 WL 6779864

End of Document © 2018 Thomson Reuters. No claim to original U.S. Government Works.

22 FCC Rcd. 6927 (F.C.C.), 22 F.C.C.R. 6927, 40 Communications Reg. (P&F) 1282, 2007 WL 983953

NOTE: An Erratum is attached to the end of this document

Federal Communications Commission (F.C.C.)
Report and Order and Further Notice of Proposed Rulemaking

IN THE MATTER OF IMPLEMENTATION OF THE TELECOMMUNICATIONS ACT OF 1996: TELECOMMUNICATIONS CARRIERS' USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION AND OTHER CUSTOMER INFORMATION

CC 96-115

IP-ENABLED SERVICES

WC 04-36
FCC 07-22
Adopted: March 13, 2007
Released: April 2, 2007
Comment Date: [30 days after publication in the Federal Register]
Reply Comment Date: [60 days after publication in the Federal Register]

**1 *6928 By the Commission: Chairman Martin issuing a separate statement; Commissioners Copps and Adelstein dissenting in part and issuing separate statements; Commissioner Tate concurring in part and issuing a separate statement; Commissioner McDowell issuing a separate statement.

I. INTRODUCTION

1. In this Order, the Commission responds to the practice of "pretexting"[1] by strengthening our rules to protect the privacy of customer proprietary network information (CPNI)[2] that is collected and held by providers of communications services (hereinafter, communications carriers or carriers).[3] Section 222 of the Communications Act requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure.[4] Today, we strengthen our privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure.

2. Our Order is directly responsive to the actions of data brokers, or pretexters, to obtain unauthorized access to CPNI. As the Electronic Privacy Information Center (EPIC) pointed out in its *6929 petition that led to this rulemaking proceeding,[5] numerous websites advertise the sale of personal telephone records for a price. These data brokers have been able to obtain private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days. The additional privacy safeguards we adopt today will sharply limit pretexters' ability to obtain unauthorized access to this type of personal customer information from carriers we regulate. We also adopt a Further Notice of Proposed Rulemaking seeking comment on what steps the Commission should take, if any, to secure further the privacy of customer information.

II. EXECUTIVE SUMMARY

3. As discussed below, we take the following actions to secure CPNI:
• **Carrier Authentication Requirements.** We prohibit carriers from releasing call detail information to customers during customer-initiated telephone contact except when the customer provides a password. If a customer does not provide a password, we prohibit the release of call detail information except by sending it to an address of record or by the carrier

WESTLAW © 2018 Thomson Reuters. No claim to original U.S. Government Works.

calling the customer at the telephone of record. We also require carriers to provide mandatory password protection for online account access. However, we permit carriers to provide CPNI to customers based on in-store contact with a valid photo ID.

2 • **Notice to Customer of Account Changes. We require carriers to notify the customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.

• **Notice of Unauthorized Disclosure of CPNI.** We establish a notification process for both law enforcement and customers in the event of a CPNI breach.

• **Joint Venture and Independent Contractor Use of CPNI.** We modify our rules to require carriers to obtain opt-in consent from a customer before disclosing a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer.

• **Annual CPNI Certification.** We amend the Commission's rules and require carriers to file with the Commission an annual certification, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI.

• **CPNI Regulations Applicable to Providers of Interconnected VoIP Service.** We extend the application of the CPNI rules to providers of interconnected VoIP service.

• **Enforcement Proceedings.** We require carriers to take reasonable measures to discover and protect against pretexting, and, in enforcement proceedings, will infer from evidence of unauthorized disclosures of CPNI that reasonable precautions were not taken.

• **Business Customers.** In limited circumstances, we permit carriers to bind themselves contractually to authentication regimes other than those adopted in this Order for services they *6930 provide to their business customers that have a dedicated account representative and contracts that specifically address the carrier's protection of CPNI.

III. BACKGROUND

A. Section 222 and the Commission's CPNI Rules

4. *Statutory Authority*. In section 222, Congress created a framework to govern telecommunications carriers' protection and use of information obtained by virtue of providing a telecommunications service.[6] The section 222 framework calibrates the protection of such information from disclosure based on the sensitivity of the information. Thus, section 222 places fewer restrictions on the dissemination of information that is not highly sensitive and on information the customer authorizes to be released, than on the dissemination of more sensitive information the carrier has gathered about particular customers.[7] Congress accorded CPNI, the category of customer information at issue in this Order, the greatest level of protection under this framework.

5. CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue *6931 of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[8] Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes some highly-sensitive personal information.

**3 6. Section 222 reflects the balance Congress sought to achieve between giving each customer ready access to his or her own CPNI, and protecting customers from unauthorized use or disclosure of CPNI. Every telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI.[9] In addition, section 222(c)(1) provides that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law;[10] (2)

with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[11] Section 222 also guarantees that customers have a right to obtain access to, and compel disclosure of, their own CPNI.[12] Specifically, pursuant to section 222(c)(2), every telecommunications carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[13]

7. *Existing Safeguards*. On February 26, 1998, the Commission released the *CPNI Order* in which it adopted a set of rules implementing section 222.[14] The Commission's CPNI rules have been amended from time to time since the *CPNI Order*, primarily in respects that do not directly impact the issues raised in this Order. Here, we focus on the substance of the Commission's rules most relevant to this Order, and briefly review the history of the creation of those rules only to the extent necessary to provide appropriate context for the actions we take today.[15]

8. In the *CPNI Order* and subsequent orders, the Commission promulgated rules implementing the express statutory obligations of section 222. Included among the Commission's CPNI regulations implementing the express statutory obligations of section 222 are requirements outlining the extent to which section 222 permits carriers to use CPNI to render the telecommunications service from which the CPNI was derived.[16] Beyond such use, the Commission's rules require carriers to obtain a customer's ***6932** knowing consent before using or disclosing CPNI. As most relevant to this Order, under the Commission's existing rules, telecommunications carriers must receive opt-out consent before disclosing CPNI to joint venture partners and independent contractors for the purposes of marketing communications-related services to customers.[17] Consistent with section 222(c)(2), the Commission's rules recognize that a carrier must comply with the express desire of a customer seeking the disclosure of his or her CPNI.[18]

9. In addition to adopting restrictions on the use and disclosure of CPNI, the Commission in the *CPNI Order* also adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.[19] Among these safeguards are rules that require carriers to design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established.[20] The Commission also requires telecommunications carriers to train their personnel as to when they are and are not authorized to use CPNI, and requires carriers to have an express disciplinary process in place.[21] The Commission's safeguard rules also require carriers to maintain records that track access to customer CPNI records. Specifically, section 64.2009(c) of the Commission's rules requires carriers to "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI," and to maintain such records for a period of at least one year.[22] The Commission's safeguard rules also require the establishment of a supervisory review process for outbound marketing campaigns.[23] Finally, the Commission requires each carrier to certify annually regarding its compliance with the carrier's CPNI requirements and to make this certification publicly available.[24]

6933 B. *IP-Enabled Services Notice

****4** 10. On March 10, 2004, the Commission initiated a proceeding to examine issues relating to Internet Protocol (IP)-enabled services -- services and applications making use of IP, including, but not limited to VoIP services.[25] In the *IP-Enabled Notice*, the Commission sought comment on, among other things, whether to extend the CPNI requirements to any provider of VoIP or other IP-enabled services.[26]

C. *EPIC CPNI Notice*

11. On August 30, 2005, EPIC filed a petition with the Commission asking the Commission to investigate telecommunications carriers' current security practices and to initiate a rulemaking proceeding to consider establishing more stringent security standards for telecommunications carriers to govern the disclosure of CPNI.[27] In particular, EPIC proposed that the Commission consider requiring the use of consumer-set passwords, creating audit trails, employing encryption, limiting data retention, and improving notice procedures.[28] On February 14, 2006, the Commission released the *EPIC CPNI Notice*, in which it sought comment on (a) the nature and scope of the problem identified by EPIC, including pretexting, and (b) what additional steps, if any, the Commission should take to protect further the privacy of CPNI.[29] Specifically, the Commission sought comment on the five EPIC proposals listed above. In addition, the Commission tentatively concluded that it should amend its rules to require carriers annually to file their section 64.2009(e) certifications with the Commission.[30] It also sought comment on whether it should require carriers to obtain a customer's opt-in consent before the carrier shares

CPNI with its joint venture partners and independent contractors; whether to impose rules relating to how carriers verify customers' identities; whether to adopt a set of security requirements that could be used as the basis for liability if a carrier failed to implement such requirements, or adopt a set of security requirements that a carrier could implement to exempt itself from liability; whether VoIP service providers or other IP-enabled service providers should be covered by any new rules the Commission adopts in the present rulemaking; and other specific proposals that might increase the protection of CPNI.

IV. DISCUSSION

12. In this Order, we adopt necessary protections put forward by EPIC to ensure the privacy of CPNI. The carriers' record on protecting CPNI demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI.[31] The Attorneys ***6934** General of dozens of states cite numerous suits by telecommunications carriers seeking to enjoin pretexting activities -- a clear indication that pretexters have been successful at gaining unauthorized access to CPNI.[32] Cingular,[33] Sprint,[34] T-Mobile,[35] Verizon Wireless[36] and other companies have sued ***6935** dozens of people whom they accuse of fraudulently obtaining phone records.[37] In one of the cases filed by Cingular, Cingular states in a court-filed affidavit that certain defendants or their agents posed as an employee/agent of Cingular and as a customer of the carrier to induce Cingular's customer service representative to provide them with the call records of a targeted customer.[38] The Federal Trade Commission has also filed suits against several pretexters under laws barring unfair and deceptive practices.[39] Additionally, numerous states, including California,[40] Florida,[41] Illinois,[42] Missouri,[43] and Texas[44] have all sued data brokers for pretexting phone records.

*6936 A. Carrier Authentication Requirements

1. Customer-Initiated Telephone Account Access

****5** 13. We find that the release of call detail[45] over the telephone presents an immediate risk to privacy and therefore we prohibit carriers from releasing call detail information based on customer-initiated telephone contact except under three circumstances.[46] First, a carrier can release call detail information if the customer provides the carrier with a pre-established password.[47] Second, a carrier may, at the customer's request, send call detail information to the customer's address of record.[48] Third, a carrier may call the telephone number of record and disclose call detail information.[49] A carrier may disclose non-call detail CPNI to a customer after the carrier authenticates the customer.[50]

***6937** 14. The record reflects that pretexters use evolving methods to trick employees at customer service call centers into releasing call detail information.[51] This release of call detail through customer-initiated telephone contact presents heightened privacy concerns because of pretexters' abilities to circumvent carrier authentication requirements and gain immediate access to call detail.[52] By restricting the ways in which carriers release call detail in response to customer-initiated telephone calls, we place at most a minimal inconvenience on carriers and consumers.[53]

15. *Establishment of Password Protection.* For new customers, carriers may request that the customer establish a password at the time of service initiation because the carrier can easily authenticate the customer at that time.[54] For existing customers to establish a password, a carrier must first authenticate the customer without the use of readily available biographical information,[55] or account information.[56] For example, a carrier could call the customer at the telephone number of record.[57] If a ***6938** carrier already has password protection in place for a customer account, a carrier does not have to reinitialize a customer password.[58] By permitting the carrier to determine its authentication method, the carrier has the most flexibility for designing an authentication program that can continue to evolve to fight against pretexting efforts.

16. *Use of Password Protection.* For accounts that are password protected, a carrier cannot obtain the customer's password by asking for readily available biographical information, or account information, to prompt the customer for his password.[59] We understand, of course, that passwords can be lost or forgotten, and share commenters' concern that security measures should not unnecessarily inconvenience customers or impair customer service systems.[60] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords that are also not based on readily available biographical information, or account information.[61] For example, the Attorneys General support the use of a shared secret back-up authentication procedure for lost or forgotten passwords.[62] As further account protection, with a shared secret back-up authentication program, the carrier may offer the opportunity for the customer to design the shared secret question.[63] We find that limiting back-up authentication methods to those that do not include readily available biographical information,

or account information, will protect customers most effectively from pretexters.

**6 *6939 17. Although we recognize that carriers and customers will be subject to a one-time burden to implement password protection if a customer is interested in gaining access to call detail during a customer-initiated telephone call, we believe that the ongoing burdens of these authentication requirements will be minimal. Further, this method balances consumers' interests in ready access to their call detail, and carriers' interests in providing efficient customer service, with the public interest in maintaining the security and confidentiality of call detail information.

18. *Alternative Access to Call Detail Information.* If a customer does not want to establish a password, the customer may still access call detail information, based on a customer-initiated telephone call, by asking the carrier to send the call detail information to an address of record or by the carrier calling the telephone number of record.[64] Because we provide multiple methods for the customer to access call detail based on a customer-initiated telephone call, neither customers who dislike passwords nor carriers concerned about timely customer service should find our requirements burdensome.[65] Furthermore, by providing a variety of secure means for customers to receive call detail information from carriers, and focusing on one of the most problematic means of pretexting -- obtaining call detail information from customer service representatives without proper identity screening -- our rules are no more extensive than necessary to protect consumers' privacy with respect to telephone access to account information.[66]

19. We do not intend for the prohibition on the release of call detail over the telephone for customer-initiated telephone contact to hinder routine carrier-customer relations regarding service/billing disputes and questions.[67] If a customer is able to provide to the carrier, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call), then the carrier is permitted to proceed with its routine customer care procedures.[68] We believe that if a customer is able to provide this information to the carrier, without carrier assistance, then the carrier does not violate our rules if it takes routine customer service actions related to such information. We additionally clarify that under these circumstances, carriers may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password. Our rule is intended to prevent pretexter phishing and other pretexter methods for gaining unauthorized access to customer account information.

***6940 2. Online Account Access**

20. We also require carriers to password protect online access to CPNI.[69] Although section 222 of the Act imposes a duty on carriers to protect the privacy of CPNI,[70] data brokers and others have been able to access CPNI online without the account holder's knowledge or consent.[71] We agree with EPIC that the apparent ease with which data brokers have been able to access CPNI online demonstrates the insufficiency of carriers' customer authentication procedures.[72] In particular, the record evidence demonstrates that some carriers permit customers to establish online accounts by providing readily available biographical information.[73] Thus, a data broker may obtain online account access easily without the customer's knowledge. Therefore, we agree with EPIC and others that use of such identifiers is an insufficient mechanism for preventing data brokers from obtaining unauthorized online access to CPNI.[74]

7 21. To close this gap, we prohibit carriers from relying on readily available biographical information, or account information to authenticate a customer's identity before a customer accesses CPNI online. In addition, because a carrier is responsible to ensure the security and privacy of online account access, a carrier must appropriately authenticate both new and existing customers seeking access ***6941 to CPNI online.[75] However, we do not require carriers to reinitialize existing passwords for online customer accounts, but a carrier cannot base online access *solely* on readily available biographical information, or account information, or prompts for such information.[76]

22. As with the password protection for the release of call detail during customer-initiated telephone contact, we understand that passwords for online access can also be lost or forgotten, and share commenters' concern that security measures should not unnecessarily inconvenience customers or impair customer service systems.[77] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords in line with the back-up authentication method framework established for the password protection for customer-initiated telephone contact.[78] Further, if a customer cannot provide a password or the proper response for the back-up authentication method to access an online account, the carrier must reauthenticate the customer based on the authentication methods adopted in this Order prior to the customer gaining online

access to CPNI.[79] Finally, as with the establishment of the password for the release of call detail for customer-initiated telephone contact, although we recognize that carriers and customers will be subject to a one-time burden to implement this Order, we believe the ongoing burdens of these authentication requirements will be minimal and are outweighed by the benefits to consumer privacy.

3. Carrier Retail Location Account Access

23. We continue to allow carriers to provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID[80] and the valid photo ID matches the name on the account.[81] We agree with the Attorneys General and find that this is a secure authentication practice because it enables the carrier to make a reasonable judgment about the customer's identity.[82]

***6942 4. Notification of Account Changes**

24. We require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication,[83] online account, or address of record is created or changed.[84] We agree with the New Jersey Ratepayer Advocate that this notification is an important tool for customers to monitor their account's security.[85] This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, as to reasonably ensure that the customer receives this notification.[86] We believe this measure is appropriate to protect customers from data brokers that might otherwise manage to circumvent the authentication protections we adopt in this Order, and to take appropriate action in the event of pretexter activity. Further, we find that this notification requirement will also empower customers to provide carriers with timely information about pretexting activity, which the carriers may not be able to identify easily.[87]

5. Business Customer Exemption

****8** 25. We do make an exception to the rules that we adopt today for certain business customers. We agree with commenters who argue that privacy concerns of telecommunications consumers are greatest when using personal telecommunications services.[88] Indeed, the fraudulent practices described by EPIC have mainly targeted individual consumers, and the record indicates that the proprietary information of wireline and wireless business account customers already is subject to stringent safeguards, which are privately negotiated by contract.[89] Therefore, if the carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact, and specifically addresses the carrier's protection of CPNI, we do not extend our carrier authentication rules to cover these business customers because businesses are typically able to negotiate the appropriate ***6943** protection of CPNI in their service agreements.[90] However, nothing in this Order exempts carriers serving wireline enterprise and wireless business account customers from section 222 or the remainder of the Commission's CPNI rules.

B. Notice of Unauthorized Disclosure of CPNI

26. We agree with EPIC that carriers should be required to notify a customer whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization.[91] However, we also appreciate law enforcement's concern about delaying customer notification in order to allow law enforcement to investigate crimes.[92] Therefore, we adopt a rule that we believe balances a customer's need to know with law enforcement's ability to undertake an investigation of suspected criminal activity, which itself might advance the goal of consumer protection.[93]

27. In conjunction with the general rulemaking authority under the Act,[94] section 222(a), which imposes a duty on "[e]very telecommunications carrier . . . to protect the confidentiality of proprietary information," provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement and prohibit them from disclosing breaches to their customers until after law enforcement has been notified. Notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI. Law enforcement can investigate the breach, which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI. When and if law enforcement determines how the breach occurred, moreover, it can advise the carrier and the Commission, enabling industry to take steps to prevent future breaches of that kind. Because law enforcement will be informed of all breaches, it will be better positioned than individual carriers to develop expertise about the methods and motives associated with CPNI breaches. Again, this should enable law

enforcement to advise industry, the Commission, and perhaps Congress regarding additional measures that might prevent future breaches.

9 28. The requirement that carriers delay customer notification of breaches until after law enforcement has been notified is also consistent with these goals. Once customers have been notified, a breach may become public knowledge, thereby impeding law enforcement's ability to investigate the **6944 breach, identify the perpetrators, and determine how the breach occurred. In short, immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches. A short delay is warranted, therefore, with the proviso that carriers may notify customers if there is an urgent need to do so to avoid immediate and irreparable harm.

29. A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).[95] A telecommunications carrier may notify the customer and/or disclose the breach publicly after seven business days following notification to the USSS and the FBI, if the USSS and the FBI have not requested that the telecommunications carrier continue to postpone disclosure.[96] A telecommunications carrier, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if the carrier believes that there is an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm.[97] Additionally, we require carriers to maintain a record of any discovered breaches, notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach.

30. We reject commenters' argument that the Commission need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure.[98] If customers and law enforcement agencies are unaware of pretexting activity, unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases.[99] By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever "next steps" are appropriate in light of the customer's particular situation.[100]

31. We clarify, however, that nothing in today's Order is intended to alter existing law regarding customer notification of law enforcement access to customer records. Therefore, for example, when CPNI is disclosed pursuant to the "except as required by law" exception contained in section 222(c)(1), such disclosure does not trigger the carrier's obligation to notify a customer of any "unauthorized" access **6945** to CPNI.[101] We further clarify that nothing in today's Order is intended to mandate customer notice when providers of covered services are permitted by law to disclose customers' personal information, such as to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[102] Further, we do not intend to supersede any statute, regulation, order, or interpretation in any state, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

**10 32. *Content of Customer Notice*. We decline to specify the precise content of the notice that must be provided to customers in the event of a security breach of CPNI. The notice requirement we adopt in this proceeding is general, and we recognize that numerous types of circumstances -- including situations other than pretexting -- could result in the unauthorized disclosure of a customer's CPNI to a third party. Thus, we leave carriers the discretion to tailor the language and method of notification to the circumstances.[103] Finally, we expect carriers to cooperate fully in any law enforcement investigation of such unauthorized release of CPNI or attempted unauthorized access to an account consistent with statutory and Commission requirements.

C. Additional Protection Measures

33. *Guarding Against Pretexting*. We agree with commenters that techniques for fraud vary and tend to become more sophisticated over time, and that carriers need leeway to engage emerging threats.[104] We therefore clarify that carriers are free to bolster their security measures through additional measures to meet their section 222 obligations to protect the privacy of

CPNI.[105] We also codify the existing statutory requirement contained in section 222 of the Act that carriers take reasonable measures to discover and protect against activity that is indicative of pretexting.[106] As we discuss below, adoption of the rules in this Order does not relieve carriers of their fundamental duty to remain vigilant in their protection of CPNI, nor does it necessarily insulate them from enforcement action for unauthorized disclosure of CPNI.

34. Although we expect that carriers will use forms of self-monitoring to comply with this obligation, at this time we allow carriers to determine what specific measures will best enable them to ***6946** ensure compliance with this requirement.[107] By codifying a general requirement to take reasonable measures to discover and protect against activity that is indicative of pretexting, we permit carriers to weigh the benefits and burdens of particular methods of possibly detecting pretexting. This approach will allow carriers to improve the security of CPNI in the most efficient manner possible,[108] and better enable small businesses to comply with our rules.

35. We stress our expectation that carriers will take affirmative measures to discover and protect against activity that is indicative of pretexting beyond what is required by the Commission's current rules,[109] and remind carriers that the Act imposes on them the duty of instituting effective measures to protect the privacy of CPNI.[110] Moreover, as discussed in the Enforcement Section, *infra*,[111] by requiring carriers to demonstrate that they have taken adequate measures to guard against pretexting, we give carriers adequate incentive to uncover situations where they have released CPNI to a third party without authorization. We anticipate that a carrier that practices willful blindness with regard to pretexting would not be able to demonstrate that it has taken sufficient measures to guard against pretexting. Although, we do not adopt specific rules in this Order that fully encompass this affirmative duty, we seek comment in our Further Notice on whether the Commission should require carriers to utilize audit trails and comply with certain data retention requirements.[112]

****11** 36. *Network Security*. In response to EPIC's encryption proposal, we make clear that carriers' existing statutory obligations to protect their customers' CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.[113] Although several carriers report that they have looked for, but not found, attempts by outsiders to penetrate their CPNI databases directly,[114] commenters also report that pretexters' methods for gaining access to data evolve over time.[115] As carriers take stronger measures to safeguard CPNI, data brokers may respond by escalating their techniques to access CPNI, such as through hacking. Therefore, although we decline at this time specifically to require carriers to encrypt their CPNI databases, we interpret section 222 as requiring carriers to protect CPNI when it is stored in a carrier's databases.[116]

***6947 D. Joint Venture and Independent Contractor Use of CPNI**

37. We modify our rules to require telecommunications carriers to obtain opt-in consent from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer.[117] While we realize that this is a change in Commission policy, we find that new circumstances force us to reassess our existing regulations. As we have found previously, the Commission has a substantial interest in protecting customer privacy.[118] Based on this and in light of new privacy concerns, we now find that an opt-in framework for the sharing of CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer both directly advances our interest in protecting customer privacy and is narrowly tailored to achieve our goal of privacy protection. Specifically, an opt-in regime will more effectively limit the circulation of a customer's CPNI by maintaining it in a carrier's possession unless a customer provides informed consent for its release. Moreover, we find that an opt-in regime will provide necessary informed customer choice concerning these information sharing relationships with other companies.

38. In the *Notice*, the Commission sought comment on whether the existing opt-out regime is sufficiently protective of the privacy of CPNI when CPNI is disclosed to telecommunications carriers' joint venture partners and independent contractors, and whether the Commission should instead adopt an opt-in policy for this type of CPNI sharing.[119] The current opt-out regime allows for carriers to share CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services after providing only a notice to a customer.[120] The burden is then placed on the customer to opt-out of such sharing arrangements. If the customer does not respond, a carrier's sharing of customer information with these entities is allowed.

****12** 39. We find that there is a substantial need to limit the sharing of CPNI with others outside a customer's carrier to

protect a customer's privacy. The black market for CPNI has grown exponentially with an increased market value placed on obtaining this data, and there is concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity.[121] The reality of this private information being disseminated is well-documented and has already resulted in irrevocable damage to customers.[122] While there are safeguards in our current rules for sharing CPNI with joint venture partners ***6948** and independent contractors,[123] we believe that these safeguards do not adequately protect a customer's CPNI in today's environment. Specifically, we find that once the CPNI is shared with a joint venture partner or independent contractor, the carrier no longer has control over it and thus the potential for loss of this data is heightened.[124] We find that a carrier's section 222 duty to protect CPNI extends to situations where a carrier shares CPNI with its joint venture partners and independent contractors. However, because a carrier is no longer in a position to personally protect the CPNI once it is shared -- and section 222's duties may not extend to joint venture partners or independent contractors themselves in all cases -- we find that this sharing of data, while still permitted, warrants a requirement of express prior customer authorization.[125]

40. We agree with commenters that argue that the current opt-out notices allowing carriers to share information with joint venture partners and independent contractors are often vague and not comprehensible to an average customer.[126] Further, we find that many consumer studies on opt-out regimes also reflect this consumer confusion.[127] We do not believe that simply modifying our existing opt-out notice requirements will alleviate these concerns because opt-out notices do not involve a customer actually authorizing the sharing of CPNI in the first instance, but rather leave it to the carrier to decide whether to share it after sending a notice to a customer, which a customer may or may not have read.[128] While many customers accept and understand that carriers will share their information with affiliates and agents -- as provided in our existing opt-out rules -- there is less customer willingness for their information to be shared without their express authorization with others outside the carrier-customer relationship.[129]

41. We disagree with commenters that assert that an opt-in approach will not serve to remedy the concerns raised in this proceeding.[130] The Attorneys General note that since February 2005, security breaches have resulted in the personal information of over 54 million Americans being compromised.[131] With the growing interest in obtaining customer CPNI and the resulting increase in the number of security breaches, carriers must be more vigilant in protecting a customer's CPNI from unauthorized disclosure.[132] It stands to reason that placing customers' personal data in the hands of companies outside the carrier- ***6949** customer relationship places customers at increased risk, not only of inappropriate handling of the information, but also of innocent mishandling or loss of control over it. Further, we find that an opt-in regime will clarify carriers' information sharing practices because it will force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization to engage in such activity.

****13** 42. We also disagree with commenters that argue that the current opt-out approach is sufficient, and that in the event of a breach, a carrier can terminate its relationship with the joint venture partner or independent contractor, or that the Commission can simply deal with the situation through an enforcement proceeding.[133] We find that in the event of a breach of CPNI security, the damage is already inflicted upon the customer. We also find that the carrier cannot simply rectify the situation by terminating its agreement nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding.[134]

43. This minor modification of our rules seeks to narrow the number of avenues available for an unauthorized disclosure of CPNI without eliminating a carrier's ability to share CPNI with its joint venture partners and independent contractors under certain circumstances. We disagree that an opt-in regime's costs outweigh the benefits to customers.[135] While we appreciate commenter concern that carriers may need to engage in broader marketing campaigns for their services as a result of an opt-in regime, we believe that this cost is outweighed by the carriers' duty to protect their customers' private information, and more importantly, customers' interest in maintaining control over their private information.[136] Thus, we believe that an opt-in regime is the least restrictive means to ensure that a customer has control over its private information and is not subjected to permanent harm as a result of a carrier's disclosure of CPNI to one of its joint venture partners or independent contractors.[137]

44. We disagree with commenters who assert that an opt-in regime for disclosures to joint venture partners and independent contractors fails the *Central Hudson* test[138] for the regulation of commercial speech.[139] We recognize that more than seven years ago, in *U.S. West, Inc. v. FCC*, the United States Court of Appeals for the Tenth Circuit held that the Commission had failed, based on the record in that proceeding, to satisfy its burden of showing that an opt-in rule passed the *Central Hudson*

test.[140] That decision, however, was based on a different record than the one compiled here and, in particular, on two premises that are no longer valid. First, the Tenth Circuit concluded that there was no evidence showing harm to privacy interests from unauthorized disclosure of CPNI. "While protecting ***6950** against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract, we have no indication of how it may occur in reality with respect to CPNI. Indeed, we do not even have indication that the disclosure might actually occur."[141] The record in this proceeding, by contrast, is replete with specific examples of unauthorized disclosure of CPNI and the adverse effects of such disclosures on customers.[142] Indeed, in the Telephone Records and Privacy Protection Act of 2006, Congress recently found that unauthorized disclosure of telephone records is a problem that "not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations."[143] Second, the Tenth Circuit in *U.S. West* concluded that the record "d[id] not adequately show that an opt-out strategy would not sufficiently protect customer privacy."[144] In this proceeding, however, substantial evidence shows that the current opt-out rules do not adequately protect customer privacy because most customers either do not read or do not understand carriers' opt-out notices.[145] For example, the National Association of Attorneys General cites to "studies [that] serve as confirmation of what common sense tells us: that in this harried country of multitaskers, most consumers are unlikely to read extra notices that arrived in today's or last week's mail and thus, will not understand that failure to act will be treated as an affirmative consent to share his or her information."[146]

****14** 45. We find, based on the record in this proceeding, that requiring carriers to obtain opt-in consent from customers before sharing CPNI with joint venture partners and independent contractors for marketing purposes satisfies the *Central Hudson* test. Specifically, we find that: (1) unauthorized disclosure of CPNI is a serious and growing problem; (2) the government has a substantial interest in preventing unauthorized disclosure of CPNI because such disclosure can have significant adverse consequences for privacy and safety;[147] (3) the more independent entities that possess CPNI, the greater the danger of unauthorized disclosure; (4) an opt-in regime directly and materially advances privacy and safety interests by giving customers direct control over the distribution of their private information outside the carrier-customer relationship; and (5) an opt-in regime is not more extensive than necessary to protect privacy and safety interests because opt-out rules, the alternative cited by the Tenth Circuit in *U.S. West, Inc. v. FCC*, do not adequately secure customers' consent for carriers to share CPNI with unaffiliated entities. In short, given the undisputed evidence demonstrating that unauthorized disclosures of CPNI constitute a serious and prevalent problem in the United States today, we believe that carriers should be required to obtain a customer's explicit consent before sending such sensitive information outside of the company for marketing purposes. In light of the serious damage that unauthorized CPNI disclosures can cause, it is important that individual consumers determine if they want to bear the increased risk associated with sharing CPNI with independent contractors and joint venture partners, and the only way to ensure that a consumer is willingly bearing that risk is to require opt-in consent. In this vein, we note that most United States privacy laws, such as the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, Video Privacy Protection Act, Driver's Privacy Protection Act, and Children's Online Privacy Protection Act, do not ***6951** employ an opt-out approach but rather require an individual's explicit consent before private information is disclosed or employed for secondary purposes.[148]

46. We disagree with commenters who contend that requiring carriers to obtain opt-in consent from customers before sharing CPNI is unnecessary because, they claim, there is no evidence that data brokers have obtained CPNI from carriers' joint venture partners and independent contractors.[149] While it is true that the record does not include specific examples of unauthorized disclosure of CPNI by a joint venture partner or independent contractor, that does not mean unauthorized disclosure has not occurred or will not occur in the future. We see no reason why joint venture partners and independent contractors would be immune from this widespread problem. While carriers argue that pretexters do not focus their efforts on independent contractors and joint venture partners, we disagree with commenters who suggest that the governmental interests at stake in this proceeding are limited to the prevention of pretexting.[150] The rules we are adopting are designed to curtail *all* forms of unauthorized disclosure of CPNI, not just pretexting. Unauthorized disclosure of CPNI by any method invades the privacy of unsuspecting consumers and increases the risk of identity theft, harassment, stalking, and other threats to personal safety.[151] In this proceeding, commenters have identified at least two other common forms of unauthorized disclosure of CPNI: computer intrusion and disclosure by insiders.[152] Indeed, evidence in the record suggests that 50-70% of cases of identity theft arise from wrongful conduct by insiders.[153] The record further demonstrates that information security breaches are on the rise in this country, and it is axiomatic that the more companies that have access to CPNI, the greater the risk of unauthorized disclosure through disclosure by insiders or computer intrusion.[154] Thus, by sharing CPNI with joint venture partners and independent contractors, it is clear that carriers increase the odds of wrongful disclosure of this sensitive

information, and before the chances of unauthorized disclosure are increased, a customer's explicit consent should be required. In any event, returning to the issue of pretexting, we also reject the argument that pretexters do not attempt to obtain CPNI from independent contractors and joint venture partners. Indeed, Sprint admits that "pretexters persist without regard to the status of any carrier representative (whether an employee, a joint venture partner, or an independent contractor)."[155] To be ***6952** sure, certain carriers claim that they do not provide the type of CPNI to joint venture partners and independent contractors that are attractive to pretexters. But even assuming this to be true for the moment, this does not appear to be the case across the entire industry.

****15** 47. Carriers also argue that there are more narrowly tailored alternatives to requiring opt-in consent for disclosures of CPNI to independent contractors and joint venture partners. First, Verizon suggests that the Commission could mandate password protection of call detail information.[156] While we agree that this is a good idea and adopt it in this Order,[157] this step is plainly insufficient by itself to address all of the legitimate privacy concerns at issue in this proceeding. Such a step, for example, would do nothing to protect the unauthorized disclosure of call detail information in the possession of independent contractors and joint venture partners by insiders or computer intrusion, let alone the unauthorized disclosure of other forms of CPNI.

48. Second, Verizon argues that it would be sufficient to adopt an opt-in regime only for call detail information shared with independent contractors and joint venture partners.[158] We likewise conclude that this alternative would be inadequate. While we recognize that unauthorized disclosure of call detail information is a significant problem, all CPNI constitutes sensitive information that is protected under the Communications Act and our rules.[159] Moreover, we note that Congress did not distinguish between call detail and non-call detail information in the Telephone Records and Privacy Protection Act of 2006.[160] Verizon's premise that non-call detail information is not sufficiently sensitive to warrant an opt-in requirement is therefore incorrect. For example, information about a customer's calling plan may be highly sensitive. T-Mobile currently offers a "myFaves" plan that allows customers to make unlimited calls to five "myFaves" contacts for a flat monthly charge, and Alltel offers a similar calling plan (the My Circle Plan) that allows for unlimited calls to ten contacts.[161] While the identity of such contacts would not constitute call detail information, such information is no doubt highly personal and would be of significant interest to those seeking to invade another's privacy. As a result, we believe that carriers should be required to obtain a customer's explicit consent before such information is shared with independent contractors or joint venture partners and thus placed at greater risk of unauthorized disclosure.

49. Finally, carriers suggest that the Commission could mandate that carriers sharing CPNI with joint venture partners and independent contractors implement additional contractual safeguards.[162] We again conclude that this alternative would not adequately vindicate our interest in protecting consumers' privacy. Further contractual safeguards would not change the fact that the risk of unauthorized CPNI disclosures increases when such information is provided by a carrier to a joint venture partner or independent contractor. Indeed, in light of the record developed in this proceeding, it is quite apparent that safeguards implemented by carriers themselves often fail to prevent unauthorized disclosures of ***6953** CPNI.[163] It is for this reason that we believe that a carrier should be required to obtain explicit consent from its customer before that customer's CPNI is sent outside of the company for marketing purposes.

****16** 50. *Grandfathering of Previously Obtained CPNI Approvals*. To the extent that carriers voluntarily obtained opt-in approval from their customers for the disclosure of customers' CPNI to a joint venture partner or independent contractor for the purposes of marketing communications-related services to a customer prior to the adoption of this Order, those carriers can continue to use those approvals.

E. Annual Certification Filing

51. We adopt the Commission's tentative conclusion and amend our rules to require carriers to file their annual CPNI certification with the Commission, including an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.[164] We find that this amendment to the Commission's rules is an appropriate measure and will ensure that carriers regularly focus their attention on their duty to safeguard CPNI. Additionally, we find that this modification to our rules will remind carriers of the Commission's oversight and high priority regarding carrier performance in this area. Further, with this filing, the Commission will be better able to monitor the industry's response to CPNI privacy issues and to take any necessary steps to ensure that carriers are managing customer CPNI securely.[165]

52. Under the Commission's existing CPNI regulations, each telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules and to make that certification available to the public.[166] While carriers currently are required to certify annually that their operating procedures are ***6954** adequate to ensure compliance with the Commission's CPNI rules, the failure of carriers to make this annual certification in their own public file, and the evidence EPIC introduced into the record regarding the industry-wide problem of pretexting, suggests that certain carriers have been less than vigilant concerning the safeguarding of CPNI.[167]

53. We find that carriers should be required to make this filing annually with the Enforcement Bureau on, or before, March 1, in EB Docket No. 06-36, for data pertaining to the previous calendar year.[168] We believe that this deadline will provide carriers with ample opportunity to review their own CPNI protection programs and ensure the adequacy of their defenses against fraudulent attempts to access customers' private data.[169] Further, this deadline will allow carriers sufficient time to review their filings without the certification being overshadowed by other annual filing requirements.

F. Extension of CPNI Requirements to Providers of Interconnected VoIP Service

54. We extend the application of the Commission's CPNI rules to providers of interconnected VoIP service.[170] In the *IP-Enabled Services Notice* and the *EPIC CPNI Notice*, the Commission sought ***6955** comment on whether to extend the CPNI requirements to VoIP service providers.[171] Since we have not decided whether interconnected VoIP services are telecommunications services or information services as those terms are defined in the Act, nor do we do so today,[172] we analyze the issues addressed in this Order under our Title I ancillary jurisdiction to encompass both types of service.[173] If the Commission later classifies interconnected VoIP service as a telecommunications service, the providers of interconnected VoIP services would be subject to the requirements of section 222 and the Commission's CPNI rules as telecommunications carriers under Title II.[174]

****17** 55. We conclude that we have authority under Title I of the Act to impose CPNI requirements on providers of interconnected VoIP service. Ancillary jurisdiction may be employed, in the Commission's discretion, when Title I of the Act gives the Commission subject matter jurisdiction over the service to be regulated[175] and the assertion of jurisdiction is "reasonably ancillary to the effective performance of [its] various responsibilities."[176] Both predicates for ancillary jurisdiction are satisfied here. First, as we concluded in the *Interim USF Order and VoIP 911 Order*, interconnected VoIP services fall within the subject matter jurisdiction granted to us in the Act.[177] Second, our analysis requires us to evaluate ***6956** whether imposing CPNI obligations is reasonably ancillary to the effective performance of the Commission's various responsibilities. Based on the record in this matter, we find that sections 222 and 1 of the Act provide the requisite nexus, with additional support from section 706.

56. Section 222 requires telecommunications carriers to protect the confidentiality of CPNI, and the Commission has adopted detailed regulations to help clarify this duty.[178] The Commission already has determined that interconnected VoIP service "is increasingly used to replace analog voice service" -- a trend that we expect will continue.[179] It therefore seems reasonable for American consumers to expect that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable.[180]

57. Moreover, extending section 222's protections to interconnected VoIP service customers is necessary to protect the privacy of wireline and wireless customers that place calls to or receive calls from interconnected VoIP customers. The CPNI of interconnected VoIP customers includes call detail information concerning all calling and called parties. Thus, by protecting from inadvertent disclosure the CPNI of interconnected VoIP customers, the Commission will more effectively protect the privacy of wireline and wireless service customers. We therefore find that the extension of the CPNI privacy requirements to providers of interconnected VoIP service is reasonably ancillary to the effective performance of the Commission's duty to protect the CPNI of all telecommunications customers under Title II.

58. Section 1 of the Act charges the Commission with responsibility for making available "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service . . . for the purpose of *promoting safety of life and property* through the use of wire and radio communication."[181] In light of this statutory mandate in conjunction with the recent real-life

implications of the unauthorized release of CPNI, protecting a consumer's private information continues to be one of the Commission's public safety responsibilities.[182] If we failed to exercise our responsibilities under sections 222 and 1 of the Act with respect to customers of interconnected VoIP service, a significant number of American consumers might suffer a loss of privacy and/or safety resulting from unauthorized disclosure of their CPNI -- and be ***6957** harmed by this loss. Therefore, we believe that extending the CPNI obligations to interconnected VoIP service providers is "reasonably ancillary to the effective performance of [our] responsibilities"[183] under sections 222 and 1 of the Act, and "will 'further the achievement of long-established regulatory goals'"[184] to protect the confidentiality of CPNI.[185]

****18** 59. We also are guided by section 706 of the Act, which, among other things, directs the Commission to encourage the deployment of advanced telecommunications capability to all Americans by using measures that "promote competition in the local telecommunications market."[186] The protection of CPNI may spur consumer demand for interconnected VoIP services, in turn driving demand for broadband connections, and consequently encouraging more broadband investment and deployment consistent with the goals of section 706.[187] Thus, pursuant to our ancillary jurisdiction, we extend the CPNI obligations to providers of interconnected VoIP services.[188]

G. Preemption

60. We reject commenter requests to preempt all state CPNI obligations[189] because we agree with commenters that assert we should allow states to also create rules for protecting CPNI.[190] We ***6958** recognize that many states already have laws relating to safeguarding personal information such as CPNI.[191] To the extent those laws do not create a conflict with federal requirements, carriers are able to comply with federal law and state law. Should a carrier find that it is unable to comply simultaneously with the Commission's rules and with the laws of another jurisdiction, the carrier should bring the matter to our attention in an appropriate petition.[192]

H. Implementation

61. In light of the importance of this issue to the public interest,[193] we require that our rules become effective within an aggressively short amount of time because of the important consumer and public safety considerations raised by pretexting that demand near immediate action.[194] The rules we adopt in this Order, however, are subject to approval by the Office of Management and Budget (OMB). Thus, our rules become effective six months after the Order's effective date or on receipt of OMB approval, as required by the Paperwork Reduction Act,[195] whichever is later. We will issue a Public Notice when OMB approval is received. For carriers satisfying the definition of a "small entity" or a "small business concern" under the Regulatory Flexibility Act or Small Business Act,[196] we provide an ***6959** additional six months to implement the rules pertaining to the online carrier authentication requirements.[197]

62. We find that the requirements we adopt in this Order most appropriately respond to actions by wrongdoers to obtain unauthorized access to CPNI, and carriers' failures to adequately protect CPNI in violation of their section 222 duty. This order balances those actions and inactions against the privacy concerns of all Americans. By requiring carriers (including interconnected VoIP service providers) to implement CPNI protections as a top priority, we hope to minimize the likelihood of future unauthorized disclosures of consumer's CPNI.

I. Enforcement

63. We take seriously the protection of customers' private information and commit to remaining vigilant to ensure compliance with applicable privacy laws within our jurisdiction. One way in which we will help protect consumer privacy is through strong enforcement measures. When investigating compliance with the rules and statutory obligations, the Commission will consider whether the carrier has taken reasonable precautions to prevent the unauthorized disclosure of a customer's CPNI. Specifically, we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue. If the Commission finds at the conclusion of its investigation that the carrier indeed has not taken sufficient steps adequately to protect the privacy of CPNI, the Commission may sanction it for this oversight, including through forfeiture.

**19 64. We offer here additional guidance regarding the Commission's expectations that will inform our investigations. We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.[198] Of course, we require carriers to implement the specific minimum requirements set forth in the Commission's rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier. For instance, and as discussed above, although we decline to impose audit trail obligations on carriers at this time, we expect carriers through audits or other measures to take reasonable measures to discover and protect against activity that is indicative of pretexting. Similarly, although we do not specifically require carriers to encrypt their customers' CPNI, we expect a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI at a cost that is reasonable given the technology a carrier already has implemented.

65. By adopting certain specific minimum standards regarding what measures carriers must take to protect the privacy of CPNI, and by committing to taking resolute enforcement action to ensure that the ***6960** goals of section 222 are achieved, we believe we appropriately balance consumer privacy interests with carriers' interests in minimizing burdens on their customers. Our two-prong approach will (1) allow carriers to implement whatever security measures are warranted in light of their technological choices, (2) create a diversity of security practices that will enable market forces to improve carriers' security measures over time, (3) avoid creating unnecessary regulatory barriers that could impede carriers from adapting to new threats as the methods used by data brokers evolve, and (4) alleviate commenters' concerns that specific safeguard rules could provide pretexters with a "roadmap" of how to obtain CPNI without authorization. We further believe that our two-pronged approach will ensure a high level of privacy protection for CPNI because carriers will have sufficient incentive and ability to adopt whatever security mechanisms work best with their existing systems and procedures.

66. *Carrier Safe Harbor.* We decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization. Some carriers support the adoption of a "safe harbor," which would immunize carriers from liability for improper disclosure of CPNI if the carrier followed certain security guidelines, such as those comparable to the Federal Trade Commission's (FTC's) guidelines for the financial industry.[199] We decline to adopt this proposal because such a rule would result in less protection of customers' CPNI than exists under the status quo. The guidelines the carriers propose to trigger immunity do not add meaningful protections beyond carriers' existing regulatory obligations.[200] Therefore, if we adopted the proposed safe harbor, carriers would receive immunity from liability for meeting the requirements set forth in the safe harbor, even if a carrier acted egregiously and in derogation of its general duty to protect CPNI from unauthorized release. The public interest is better served if the Commission retains the option of taking strong enforcement measures regarding carriers' duties under section 222 and the Commission's rules.

V. FURTHER NOTICE OF PROPOSED RULEMAKING

**20 67. The Commission has a duty to ensure that, as technologies evolve, the consumer protection objectives of the Act are maintained. Through this Further Notice of Proposed Rulemaking, we seek comment on whether the Commission should act to expand its CPNI rules further, and whether it should expand the consumer protections to ensure that customer information and CPNI are protected in the context of mobile communication devices.

A. Additional CPNI Protective Measures

68. *Password Protection.* In light of the rules we adopt in today's Order and the recent enactment of criminal penalties against pretexters, we seek comment on whether the Commission should adopt any further carrier requirements to protect CPNI. Specifically, while we limited our rules to password protecting call detail information for customer-initiated telephone contact, we seek comment on whether to extend these rules to include optional or mandatory password protection for non-call detail CPNI. Should this password protection be for all non-call detail CPNI or should it only include certain account changes? Further, if the Commission were to adopt password protection for certain account changes, what should that include (*e.g.*, changes in the address of record, account plans, or billing methods)? Would requiring these forms of password protection place an undue burden on carriers, ***6961** customers, or others, including any burdens placed on small carriers? We solicit further comment on any other modifications to our rules that we should adopt in light of pretexting activity, and a carrier's duty to protect CPNI.

69. *Audit Trails.* While we did not adopt rules requiring audit trails at this time, in light of our new rules and the recent enactment of criminal penalties against pretexters, we seek comment on whether the Commission should adopt rules pertinent to audit trails. Are audit trails generally used by carriers to track customer contact? We ask carriers to assess the benefits and burdens, including the burdens on small carriers, of recording the disclosure of CPNI and customer contact. Our current record indicates that the broad use of audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate customer inquiry.[201] Commenters also report that implementing and maintaining audit trails would be costly with little to no corresponding benefit to the consumer.[202] However, would an audit trail assist law enforcement with its criminal investigations against pretexters? Further, in the interim period since we sought comment on this issue, have carriers' reactions to audit trails changed or has the technology changed such that audit trails are now an economically feasible option?

70. *Physical Safeguards.* We also seek comment on whether the Commission, in light of the rules we adopt in this Order and the recent enactment of criminal penalties against pretexters, should adopt rules that govern the physical transfer of CPNI among companies, such as between a carrier and its affiliates, or the transfer of CPNI to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. Specifically, we seek comment on what physical safeguards carriers currently are using when they transfer, or allow access to, CPNI to ensure that they maintain the security and confidentiality of CPNI?[203] We also seek comment on whether these safeguards for the physical transfer of, or for access to, CPNI are sufficient? Further, we seek comment on what steps the Commission should require of a carrier to protect CPNI when CPNI is being transferred or accessed by the carrier, its affiliates, or its third parties (*e.g.*, encryption, audit trails, logs, etc.). Additionally, we seek comment on the benefits and burdens, including the burdens on small carriers, of requiring carriers to physically safeguard the security and confidentiality of CPNI.

21 71. *Limiting Data Retention.* We also seek comment on whether the Commission, in light of the rules we adopt in this Order and the recent enactment of criminal penalties against pretexters, should adopt rules that require carriers to limit data retention. If the Commission did adopt such a rule, what should be the maximum amount of time that a carrier should be able to retain customer records? Additionally, should all customer records be eliminated or is there a subset of customer records that are more susceptible to abuse and should be destroyed? Also, should the Commission define exceptions where a carrier is permitted to retain certain records (*e.g.*, for the length of carrier-carrier or carrier-customer disputes)? The Department of Justice argues that destruction of CPNI after a specified period would hamper law enforcement efforts by destroying data sometimes needed for criminal and other lawful investigations.[204] We also seek comment on whether there are any state or Commission data ***6962 retention requirements that might conflict with a carrier's data limitation.[205] Additionally, does a limitation on data retention enhance protection of CPNI?[206] Alternatively, should the Commission require carriers to de-identify customer records after a certain period?[207] We seek comment on the benefits and burdens, including the burdens on small carriers, of requiring carriers to limit their data retention or to de-identify customer records.

B. Protection of Information Stored in Mobile Communications Devices

72. We seek comment on what steps the Commission should take, if any, to secure the privacy of customer information stored in mobile communications devices.[208] Specifically, we seek comment on what methods carriers currently use, if any, for erasing customer information on mobile equipment prior to refurbishing the equipment,[209] and the extent to which carriers enable customers to permanently erase their personal information prior to discarding the device. We also seek comment on whether the Commission should require carriers to permanently erase, or allow customers to permanently erase, customer information in such circumstances. Should the Commission require manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from those devices? Further, we seek comment on the burdens, including those placed on small carriers, associated with a Commission rule requiring carriers and manufacturers to fully expunge existing customer data from a mobile device at the customer's request.

VI. PROCEDURAL MATTERS

A. *Ex Parte* Presentations

73. The rulemaking this Notice initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[210] Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed.

More than a one or two sentence description of the views and arguments presented generally is required.[211] Other requirements pertaining to oral and written presentations are set forth in section 1.1206(b) of the Commission's rules.[212]

***6963 B. Comment Filing Procedures**

****22** 74. Pursuant to sections 1.415 and 1.419 of the Commission's rules,[213] interested parties may file comments and reply comments regarding the Notice on or before the dates indicated on the first page of this document. **All filings related to this Further Notice of Proposed Rulemaking should refer to CC Docket No. 96-115 and WC Docket No. 04-36.** Comments may be filed using: (1) the Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies. See Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://www.fcc.gov/cgb/ecfs/ or the Federal eRulemaking Portal: http://www.regulations.gov. Filers should follow the instructions provided on the website for submitting comments.
- ECFS filers must transmit one electronic copy of the comments for CC Docket No. 96-115 and WC Docket No. 04-36. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and the applicable docket number. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions, filers should send an e-mail to ecfs@fcc.gov, and include the following words in the body of the message, "get form." A sample form and directions will be sent in response.

- Paper Filers: Parties who choose to file by paper must file an original and four copies of each filing. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail). All filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.
- The Commission's contractor will receive hand-delivered or messenger-delivered paper filings for the Commission's Secretary at 236 Massachusetts Avenue, N.E., Suite 110, Washington, D.C. 20002. The filing hours at this location are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

- U.S. Postal Service first-class, Express, and Priority mail should be addressed to 445 12th Street, S.W., Washington D.C. 20554.

75. Parties should send a copy of their filings to Janice Myles, Competition Policy Division, Wireline Competition Bureau, Federal Communications Commission, Room 5-C140, 445 12th Street, S.W., Washington, D.C. 20554, or by e-mail to janice.myles@fcc.gov. Parties shall also serve one copy with the Commission's copy contractor, Best Copy and Printing, Inc. (BCPI), Portals II, 445 12th Street, S.W., Room CY-B402, Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

****23** 76. Documents in CC Docket No. 96-115 and WC Docket No. 04-36 will be available for public inspection and copying during business hours at the FCC Reference Information Center, Portals II, 445 12th Street S.W., Room CY-A257, Washington, D.C. 20554. The documents may also be purchased ***6964** from BCPI, telephone (202) 488-5300, facsimile (202) 488-5563, TTY (202) 488-5562, e-mail fcc@bcpiweb.com.

C. Final Regulatory Flexibility Analysis

77. As required by the Regulatory Flexibility Act of 1980, see 5 U.S.C. § 604, the Commission has prepared a Final

Regulatory Flexibility Analysis (FRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The FRFA is set forth in Appendix C.

D. Initial Regulatory Flexibility Analysis

78. As required by the Regulatory Flexibility Act of 1980, see 5 U.S.C. § 603, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The IRFA is set forth in Appendix D. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Notice provided below in Appendix D.

E. Paperwork Reduction Act

79. This Order contains modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new information collection requirements contained in this proceeding. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

80. In the Order, we have assessed the burdens placed on small businesses to notify customers of account changes, to notify law enforcement and customers of unauthorized CPNI disclosure; to obtain opt-in consent prior to sharing CPNI with joint venture partners and independent contractors; to file annually a CPNI certification with the Commission, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI, and to extend the CPNI rules to providers of interconnected VoIP services, and find that these requirements do not place a significant burden on small businesses.

24 81. This Further Notice contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invited the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this Further Notice, as required by the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. Public and agency comments are due **60 days after publication in the Federal Register. Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we seek comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

***6965 F. Congressional Review Act**

82. The Commission will send a copy of this Report and Order and Further Notice of Proposed Rulemaking in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act (CRA), *see* 5 U.S.C. § 801(a)(1)(A).

G. Accessible Formats

83. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice) or 202-418-0432 (TTY). Contact the FCC to request reasonable accommodations for filing comments (accessible format documents, sign language interpreters, CART, etc.) by e-mail: FCC504@fcc.gov; phone: 202-418-0530 or TTY: 202-418-0432.

VII. ORDERING CLAUSES